Office of Personnel Management (OPM) Data Breach

A briefing for use by DON commanders and supervisory staff

http://www.secnav.navy.mil/OPMBreachDON

Command Talking Points

- In the spring of 2015, the Office of Personnel Management (OPM) became aware of unprecedented compromises to government employee personal data.

- While the full scope of the data breaches is unknown, at a minimum they impact current and former federal employees including Department of the Navy (DON) personnel.

- OPM, DHS, and the FBI are continuing to investigate the extent of these intrusions. We fully expect the list of affected employees to grow as a result of this investigation. It may include a significant number of current and former military members and their families.

- While the spectrum of risk to affected individuals is also unknown, it is reasonable to assume it includes identify theft at a minimum.

- The DON recognizes the seriousness of these breaches and will provide you access to timely and accurate information as it becomes available at http://www.secnav.navy.mil/OPMBreachDON .

- Service Members, Civilians, Contractors and to be proactive, pay attention and remain vigilant. Report any suspicious activity to your chain of command.

Background

- OPM believes the **first intrusion** into its systems occurred in December 2014, and became aware of the incident in April 2015. OPM then became aware of a **second intrusion** into its systems in May 2015.

- OPM estimates that **at a minimum, these breaches affect millions of current and former government employees**. Since investigations are ongoing, additional Personally Identifiable Information (PII) exposures will likely come to light. If OPM determines that more individuals have been impacted, they will conduct additional notifications.

- OPM maintains personnel records for the federal workforce. **The kind of data that may have been compromised in these incidents is sensitive.** Compromised data may include information within background investigations, job assignments, training records and benefit selection decisions. At a minimum, this could include: name, Social Security Number, date and place of birth, and current and former addresses.

Notification Process for Incident #1 Affected Civilian Employees

- Email from OPMcio@csid.com for all current employees.
  - Be sure to check Junk folders.
- US Mail for invalid email addresses and retirees.
- Automatically enrolled for 18 months of free identity theft insurance up to $1M from CSID.
- Voluntary sign up with PIN (PIN provided in notification email/letter) for additional free credit monitoring services for 18 months.

Similar notifications are expected for Incident # 2 affected individuals as they are identified.

Table of Resources Potentially Affected Individuals

Resource	Contact Info	Provides
CSID® Credit Monitoring Service	www.csid.com/opm/ U.S. toll free: 844-777-2743 International call collect: 512-327-0700	**Assistance with signing up for CSID credit monitoring services for affected individuals.**
Department of Navy FAQ E-mail	DONhrFAQ@navy.mil	**Answers to data breach related questions.**
Department of the Navy Civilian Employee Assistance Program (DONCEAP)	www.DONCEAP.foh.hhs.gov Toll free: 1-844-DONCEAP (1-844-366- 2327) TTY: 1-888-262-7848 International: 001-866-829-0270	**Support for financial issues and identity theft for all DON civilians and their families.**
Federal Trade Commission (FTC) Complaint Submission	www.ftccomplaintassistant.gov Toll free: 1-877-ID-THEFT (438-4338)	**A clearinghouse for complaints by victims of identity theft.**
Federal Trade Commission (FTC) Identity Theft Recovery Plan	Downloadable PDF: www.identitytheft.gov	**A step by step guide on what to do if your identity information has been stolen.**
Free Credit Report Review	www.AnnualCreditReport.com Call: 1-877-322-8228	**One free credit report per year from each of the three major crediting bureaus (contact information for credit bureaus can be found on the Federal Trade Commission website: www.ftc.gov).**
Guide to Keeping Your Social Media Accounts Secure	www.doncio.navy.mil/ContentView.aspx?id=5950	**Safety guidelines and tips to keeping your personal information safe while using social media.**
Internal Revenue Service (IRS)	http://www.irs.gov/Help-&-Resources Toll free: 1-800- 908-4490	**Guidance on what to do if you suspect the improper use of identification information in connection with tax violations.**
Phishing Reports	NMCS_SPAM@navy.mil	**Resource to report phishing attempts.**
Social Security Administration	www.socialsecurity.gov/kc/id_resources.htm	**Guidance on what to do if you suspect your Social Security number is being fraudulently used.**
	Toll free: 1-800-269-0271 www.transunion.com/fraud	**Placing fraud alert on your credit file to let**